Fortify Rulepacks Version 2016.4 Released

This VA Software Assurance Notification is about the release of updated Hewlett Packard Enterprise (HPE) Security Fortify Static Code Analyzer (SCA) rulepacks, **version 2016.4**.

Scanning source code for potential vulnerabilities using HPE Fortify SCA is an authorization requirement that is enforced as part of the Authority to Operate (ATO) issuance process.

Fortify scans that do not use these new rulepacks will result in scan issues in validation submission packages accepted after **December 27, 2016**

With this release, the Fortify Secure Coding Rulepacks detect 733 unique categories of vulnerabilities across 23 programming languages and span over 850,000 individual APIs. In summary, the release includes the following:

.NET 4.6.2 enhancements1
Improved rule coverage for .NET 4.6.2 spans more than 12 namespaces and adds support for asynchronous APIs. Supported categories impacted by the improvements include the following:

- Access Control: LDAP
- Connection String Parameter Pollution
- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- Cross-Site Scripting: Inter-Component Communication (Cloud)
- Denial of Service
- Header Manipulation
- LDAP Injection
- LDAP Manipulation
- Log Forging
- Path Manipulation
- Privacy Violation
- Server-Side Request Forgery
- System Information Leak
- System Information Leak: Internal
- System Information Leak: External

In addition, coverage has been improved to detect Hardcoded, Empty, Null, and Weak Cryptography passwords under the Password Management category. Finally, two categories are added to detect insecure email and plain text password transmission in ASP.NET applications.

- Insecure Transport: Mail Transmission
- Password Management: Plain Text Password in Transit

iOS HealthKit
New support for the HealthKit framework, for both Objective-C and Swift languages. Sensitive health information is now tracked and if found to be leaked by the application, a new category will be reported: Privacy Violation: Health Information.

iOS enhancements2
This release includes improved coverage of iOS frameworks, including new support for Touch ID and iOS Extensions. Rulepacks now support 24 additional categories in both Objective-C, and Swift, to improve detection capabilities in the areas of Biometric Authentication, Header Manipulation, Input Interception, Insecure IPC, Insecure SSL, Insecure Storage, Insecure Transport, Link Injection, Privacy Violation, and Trust Boundary Violation. New categories include the following:

- Biometric Authentication: Insecure Touch ID Implementation
- Biometric Authentication: Insufficient Touch ID Protection
- Biometric Authentication: Missing Operation Message
- Header Manipulation
- Input Interception: Keyboard Extensions Allowed
- Insecure IPC: Missing Content Validation
- Insecure IPC: Missing Sender Verification
- Insecure IPC: Missing URL Validation
- Insecure IPC: URL Scheme Hijacking
- Insecure SSL: Server Identity Verification Disabled
- Insecure Storage: Externally Available Keychain
- Insecure Storage: HTTP Response Cache Leak
- Insecure Storage: Insufficient Cache Leak Protection
- Insecure Storage: Insufficient Keychain Protection
- Insecure Storage: Lacking Keychain Protection
- Insecure Storage: Passcode Policy Unenforced
- Insecure Storage: Unspecified Keychain Access Policy
- Insecure Transport: Weak SSL Protocol
- Link Injection: Auto Dial
- Link Injection: Missing Validation
- Privacy Violation: iCloud Synchronized Credentials

- Privacy Violation: Incomplete Credential Removal
- Privacy Violation: Sensitive Data Accessible From iTunes
- Trust Boundary Violation

Apache Commons Lang3
Java rulepacks now include support for Apache Commons Lang3 library which provides helper classes for manipulating strings, numerical values, object reflection, concurrency, creation, serialization, and system properties.